JOURNAL OF ALGEBRA 4, 426-432 (1966)

The Automorphism Group of Finite p-groups

HANS LIEBECK
University of Keele, Keele, Staffordshire, England

Communicated by P. Hall
Received October 14, 1965

It is well known [2; Theorem 12.2.2] that if G is a finite p-group with Frattini subgroup Φ, then the group $\mathfrak{F}$ of automorphisms of G fixing G/Φ elementwise is a finite p-group and therefore nilpotent. In this paper we shall obtain an upper bound for the nilpotency class of $\mathfrak{F}$ (Theorem 3). This is done by relating a certain central series of G to a central series of $\mathfrak{F}$. The argument uses induction (Theorem 2 giving information about the center of $\mathfrak{F}$) and depends on a partly well-known general result (Theorem 1 and Corollary 1) showing how certain subgroups of a group lead to normal subgroups of its group of automorphisms. We conclude by applying the theory to Abelian p-groups, wreath products, etc.

PRELIMINARIES

We shall use the commutator notation: $[x, y] = x^{-1}y^{-1}xy$. Let G be a group. If H is a normal subgroup of G we shall write $H \lhd G$. Denote the automorphism group of G by Aut G.

Let M be a subgroup of G. We call the automorphism μ of G an M-automorphism if $g^{-1}g^{\mu} \in M$ for all $g \in G$. Denote the set of all M-automorphisms of G by Aut $(G; M)$. This is clearly a subgroup of Aut G. Conversely, any subgroup $\mathfrak{B}$ of Aut G can be regarded as a group of M-automorphisms for various choices of M. [In particular, we can always choose $M = G$, since Aut $(G; G) =$ Aut G.] Among all the choices there is a unique minimal subgroup $K(G; \mathfrak{B}) = gp\{g^{-1}g^{\beta}; \beta \in \mathfrak{B}, g \in G\}$. Kaloujnine [5; Satz 1] proved that $K(G; \mathfrak{B}) \lhd G$. Note that $\mathfrak{B}$ may be a proper subgroup of the group of all $K(G; \mathfrak{B})$-automorphisms. For example, if G is the direct product of two cyclic groups of order 4, generated by a and b, say, and if $\mathfrak{B}$ is the group of automorphisms consisting of the identity and β, defined by $a^{\beta} = ab^2$, $b^{\beta} = b$, then $K = K(G; \mathfrak{B}) = gp\{b^2\}$ and $\mathfrak{B}$ is a proper subgroup of Aut $(G; K)$, which has order 4.

Note that if $M \lhd G$, then Aut $(G; M)$ consists of the subgroup of automorphisms in Aut G leaving G/M elementwise fixed.

Main Results

THEOREM 1. *Let M be a subgroup of a group G. Let $\mathfrak{M} = Aut(G; M)$. If N is an $\mathfrak{M}$-admissible subgroup of M, then $\mathfrak{N} = Aut(G; N) \lhd \mathfrak{M}$.*

Further, $\mathfrak{M}/\mathfrak{N}$ is isomorphic to the subgroup of automorphisms in $Aut(G/K; M/K)$ that can be extended to automorphisms of G, where $K = K(G; \mathfrak{N})$.

If $N \lhd G$, then K can be replaced by N in the above statement.

Proof. For $g \in G$, $\mu \in \mathfrak{M}$, $\nu \in \mathfrak{N}$,

$$g^{-1}g^{\mu\nu\mu^{-1}} = g^{-1}(g^{\mu}n)^{\mu^{-1}} \text{ for some } n \in N$$
$$= n^{\mu^{-1}} \in N, \text{ since } N \text{ is } \mathfrak{M}\text{-admissible.}$$

Therefore $\mu\nu\mu^{-1} \in \mathfrak{N}$, and so $\mathfrak{N} \lhd \mathfrak{M}$.

To prove the second part, note first that K is a (normal) $\mathfrak{M}$-admissible subgroup of G. For K is generated by elements of the form $g^{-1}g^{\nu}$, $\nu \in \mathfrak{N}$, and for $\mu \in \mathfrak{M}$

$$(g^{-1}g^{\nu})^{\mu} = (g^{\mu})^{-1}(g^{\mu})^{\nu^*}, \qquad \text{where } \nu^* = \mu^{-1}\nu\mu \in \mathfrak{N}.$$

Thus $(g^{-1}g^{\nu})^{\mu} \in K$.

Clearly $\mu \in \mathfrak{M}$ induces an automorphism $\bar{\mu}$ in G/K, defined by

$$(gK)^{\bar{\mu}} = g^{\mu}K = gm\,K \qquad \text{for some } m \in M.$$

We see that $\bar{\mu}$ is an M/K-automorphism of G/K. The mapping $\mu \to \bar{\mu}$ defines a homomorphism of $\mathfrak{M}$ into $\mathrm{Aut}(G/K; M/K)$. The kernel of this homomorphism is $\mathfrak{N}$, for

$$\bar{\mu} = \bar{1} \Leftrightarrow g^{-1}g^{\mu} \in K \text{ for all } g \in G$$
$$\Leftrightarrow \mu \in \mathrm{Aut}(G; K).$$

But $\mathrm{Aut}(G; K) = \mathfrak{N}$. For by definition of $K(= K(G; \mathfrak{N}))$, $\mathrm{Aut}(G; K) \supseteq \mathfrak{N}$; conversely, since $K \subseteq N$, $\mathrm{Aut}(G; K) \subseteq \mathrm{Aut}(G; N) = \mathfrak{N}$.

The last statement is proved by replacing K by N in the above argument.

Remark. As mentioned above, if $\mathfrak{N} = \mathrm{Aut}(G; N)$ and $K = K(G; \mathfrak{N})$, then $K \subseteq N$. The inclusion may be proper even if $N \lhd G$. For example, let $G = N$ be a cyclic group of order 4. Then $K(G; \mathfrak{N})$ is the subgroup of order 2.

Putting $M = G$ in Theorem 1, we have the well-known corollary:

COROLLARY 1. *If N is a characteristic subgroup of G, then $\mathfrak{N}(= Aut(G; N)) \lhd Aut\ G$, and $(Aut\ G)/\mathfrak{N}$ is isomorphic to the subgroup of automorphisms in $Aut(G/N)$ that can be extended to automorphisms of G.*

We shall now apply the above results to the case that G is a finite p-group with Frattini subgroup Φ. Let $\mathfrak{F} = \mathrm{Aut}(G; \Phi)$. Then $\mathfrak{F}$ is precisely the group of all automorphisms of G fixing G/Φ elementwise. Putting $M = \Phi$ in Theorem 1, we shall show in the following theorem how to choose $N \subseteq \Phi$ so that $\mathfrak{N}$ is contained in the center of $\mathfrak{F}$. This will serve as a basis for an induction argument to obtain (in Theorem 3) an upper bound for the nilpotency class of $\mathfrak{F}$.

THEOREM 2. *Let G be a finite d-generator p-group with lower central series $G = \Gamma_1 \supset \cdots \supset \Gamma_c \supset \Gamma_{c+1} = 1$ and $\Phi \neq 1$. Let Γ_c have exponent p^m. If $N = \Gamma_c^{p^{m-1}}$, the group generated by all (p^{m-1})th powers of elements of Γ_c, then*

(i) *N is elementwise fixed by all automorphisms in $\mathfrak{F}$;*

(ii) *$\mathfrak{N} = \mathrm{Aut}(G; N) \subseteq$ center of $\mathfrak{F}$;*

(iii) *$\mathfrak{N}$ has order p^{rd}, where p^r is the order of N;*

(iv) *$\mathfrak{F}/\mathfrak{N}$ is isomorphic to the subgroup of automorphisms in $\mathrm{Aut}(G/N; \Phi/N)$ that can be extended to automorphisms of G.*

The proof of 2(i) requires two lemmas.

LEMMA 1. *With G as in Theorem 2, if $\phi \in \mathfrak{F}$ and $a \in \Gamma_i$ $(i = 1,\ldots, c)$, then $a^\phi \equiv ah^p \bmod \Gamma_{i+1}$ for some $h \in \Gamma_i$.*

Proof. The result is clearly true for $i = 1$, since Φ/Γ_2 consists of all pth powers in G/Γ_2. Proceeding by induction on i, assume the validity of the lemma if $i < j$. Let $a \in \Gamma_j$. Then a is a product of terms $b = [y, g]$ with $y \in \Gamma_{j-1}$. Now

$$b^\phi = [y^\phi, g^\phi] = [y^\phi, gw^p x] \text{ for some } w \in G,\ x \in \Gamma_2$$
$$\equiv [y^\phi, g][y^\phi, w]^p [y^\phi, x] \bmod \Gamma_{j+1}.$$

The last step follows from well known commutator relations and the fact that $y^\phi \in \Gamma_{j-1}$. Further,

$$[y^\phi, x] \in [\Gamma_{j-1}, \Gamma_2] \subseteq \Gamma_{j+1} \text{ (see [2; Corollary 10.3.5])}.$$

By the induction hypothesis, $y^\phi = yu^p k$ for some $u \in \Gamma_{j-1}$, $k \in \Gamma_j$. Hence

$$[y^\phi, g] \equiv [y, g][u, g]^p \bmod \Gamma_{j+1}.$$

Noting that $[y^\phi, w]$ and $[u, g]$ are elements of Γ_j, and denoting their product by h, we obtain

$$b^\phi \equiv bh^p \bmod \Gamma_{j+1},\ h \in \Gamma_j,$$

and the lemma follows.

LEMMA 2. *Let N be an elementary Abelian subgroup of the center of a finite p-group G. Then every automorphism $\nu \in Aut(G; N)$ leaves Φ elementwise fixed.*

Proof. Clearly ν leaves fixed every commutator and every pth power of G. Hence Φ is left elementwise fixed.

Proof of Theorem 2. (i): If $c = 1$, that is, if G is Abelian, the result is immediate, for by Lemma 1, if $\phi \in \mathfrak{F}$ then $(a^{p^{m-1}})^\phi = (ah^p)^{p^{m-1}} = a^{p^{m-1}}$.

Suppose next that $c > 1$. Γ_c is generated by elements of the form $z = [a, g]$, $a \in \Gamma_{c-1}$. We must prove that if $k = z^{p^{m-1}}$ and $\phi \in \mathfrak{F}$, then $k^\phi = k$. Now

$$\begin{aligned}
k^\phi &= [a^\phi, g^\phi]^{p^{m-1}} \\
&= [ah^p, g^\phi]^{p^{m-1}} \text{ for some } h \in \Gamma_{c-1}, \text{ by Lemma 1,} \\
&= [a, g^\phi]^{p^{m-1}}[h, g^\phi]^{p^m}, \text{ since } a, h \in \Gamma_{c-1} \text{ and } \Gamma_{c+1} = 1, \\
&= [a, g^\phi]^{p^{m-1}} \text{ by definition of } m, \\
&= [a, gw^p x]^{p^{m-1}} \text{ for some } x \in \Gamma_2, \text{ by Lemma 1,} \\
&= [a, g][a, w]^{p^m}[a, x]^{p^{m-1}}, \\
&= [a, g] = k, \text{ for } [a, x] \in [\Gamma_{c-1}, \Gamma_2] \subseteq \Gamma_{c+1} = 1.
\end{aligned}$$

(ii): Let $\nu \in \mathfrak{N}, \phi \in \mathfrak{F}$, $g \in G$. Then

$$\begin{aligned}
g^{\nu\phi} &= (gn)^\phi \quad \text{for some } n \in N, \\
&= g^\phi n \quad \text{by Theorem 2(i)} \\
&= ghn \quad \text{for some } h \in \Phi,
\end{aligned}$$

and

$$g^{\phi\nu} = (gh)^\nu = g^\nu h^\nu = gnh^\nu = gnh \text{ (by Lemma 2)} = ghn$$

since n is contained in the center of G. Thus $\nu\phi = \phi\nu$.

(iii): If $g_1, \ldots, g_d$ generate G and $n_1, \ldots, n_d$ are arbitrary elements of N (possibly with repetitions) then the mapping $g_i \to g_i n_i$ $(i = 1, \ldots, d)$ defines an automorphism of G. We proved this in [6]. Thus $\mathrm{Aut}(G; N)$ has the maximum possible order, which is $(p^r)^d$.

(iv) follows at once from Theorem 1 with $M = \Phi$.

THEOREM 3. *Let G be as in Theorem 2, with $\Phi \neq 1$, and let Γ_i/Γ_{i+1} have exponent p^{m_i} $(i = 1, \ldots, c)$. Let $\lambda(G) = (\sum_{i=1}^{c} m_i) - 1$. Then $\mathfrak{F} = Aut(G; \Phi)$ is nilpotent of class $\leqslant \lambda(G)$.*

Proof. The possibility $\lambda(G) = 0$ is ruled out by the assumption that

$\Phi \neq 1$, which ensures that $\mathfrak{F}$ is nontrivial [Theorem 2(iii)]. If G is such that $\lambda(G) = 1$, then $c = 1$, $m_1 = 2$ or $c = 2$, $m_1 = m_2 = 1$. In either case Φ has exponent p and is contained in the center of G. Hence, putting $N = \Phi$ in Theorem 2(ii), we see that $\mathfrak{F}$ is Abelian, that is, $\mathfrak{F}$ has class $1 = \lambda(G)$. We thus have a basis for an induction argument on $\lambda(G)$. Let G be as in the statement of Theorem 3. Put $N = (\Gamma_c)^{p^{m_c-1}}$. Then by Theorem 2, $\mathfrak{N} = \text{Aut}\ (G; N) \subseteq$ center of $\mathfrak{F}$, and $\mathfrak{F}/\mathfrak{N}$ is isomorphic to a subgroup of Aut $(G/N; \Phi/N)$. Now $\lambda(G/N) = \lambda(G) - 1 < \lambda(G)$. Thus we may assume that $\text{Aut}(G/N; \Phi/N)$ is nilpotent of class $\leqslant \lambda(G/N)$. Hence $\mathfrak{F}$ is nilpotent of class $\leqslant \lambda(G/N) + 1 = \lambda(G)$, and the proof is complete.

Theorem 3 can also be proved by applying Lemma 1 to Hall's Lemma 3.5 [3]. (The lemma states that if $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = 1$ is a series of normal subgroups of G and if $\mathfrak{A}$ is the group of all automorphisms of G which leave each G_i invariant and transform each G_{i-1}/G_i identically, then $\mathfrak{A}$ is nilpotent of class $< r$.)

Some Applications

The upper bound for the class of $\mathfrak{F}$ given in Theorem 3 is most likely best possible. This is certainly the case when $c = 1$, or when $c > 1$, $m_i = 1$ $(i = 1,..., c)$ as the following two examples show.

Corollary 2. *Let $M_n(p^m)$ be the group of all $n \times n$ matrices $x = (x_{ij})$ with coefficients in the ring of integers modulo p^m and such that $x_{ij} \equiv 0 \pmod p$ whenever $i \neq j$ and $x_{ii} \equiv 1 \pmod p (i = 1,..., n)$. Then for $n \geqslant 2$, $M_n(p^m)$ is nilpotent of class $m - 1$.*

Proof. Note that $M_n(p^m)$ is isomorphic to $\text{Aut}(G; \Phi)$, where G is the direct product of n cyclic groups each of order p^m. Thus, by Theorem 3, $M_n(p^m)$ is nilpotent of class $\leqslant m - 1$. Consider the following matrices x_r for $r = 0, 1,..., m - 1$:

$$\begin{aligned} (x_r)_{ii} &= 1 \ (i = 1,..., n), \\ (x_r)_{21} &= p^r + p^{r+1} + \cdots + p^{m-1}, \\ (x_r)_{ij} &= 0 \text{ otherwise.} \end{aligned}$$

The elements of x_r^{-1} are the same as those for x_r except that $(x_r^{-1})_{21} = -(x_r)_{21}$.

Let y be the diagonal $n \times n$ matrix with $y_{22} = 1 - p + p^2 - \cdots + (-1)^{m-1}p^{m-1}$ and $y_{ii} = 1$ $(i \neq 2)$. If x_m denotes the identity matrix, then

$$[x_r, y] = x_{r+1} \ (r = 0, 1,..., m - 1).$$

Hence $M_n(p^m)$ has class $m - 1$.

COROLLARY 3. *Let G be the wreath product of a cyclic group A of prime power order p^r by a cyclic group B of order p^s, but ruling out the case $p = 2$, $r = s = 1$. Then*

(i) *Aut $G/\mathfrak{F}$ is isomorphic to a direct product of two cyclic groups of order $p - 1$. In particular, if $p = 2$ then Aut $G = \mathfrak{F}$.*

(ii) *If $r = 1$, p any prime, then $\mathfrak{F}$ is nilpotent of class $p^s - 1$.*

Proof. It is convenient to use the notation introduced in [7; 2.1]: Let A_i be an isomorphic copy of A ($i = 0,..., p^s - 1$) generated by a_i of order p^r. Identify A_i with A_j whenever $j - i$ is a multiple of p^s. If B is generated by b, the wreath product $G = A \; Wr \; B$ is defined by

$$G = gp\{B, A_i ; b^{-1}a_ib = a_{i+1} \; (i = 0,..., p^s - 1), \; [a_i, a_j] = 1, \text{ all } i, j\}.$$

(i): We shall examine which automorphisms of G/Φ can be extended to automorphisms of G and apply Corollary 1 with $N = \Phi$. Houghton [4; Theorem 3.3] showed that Aut G is expressible as a product of three subgroups, the first leaving B elementwise fixed, the second being a group of inner automorphisms (i.e., G'-automorphisms) and the third being extensions of automorphisms β of B ($b^\beta = b^k$, $(k, p) = 1$) to automorphisms β^* of G defined by

$$b^{\beta^*} = b^k, \; a_i^{\beta^*} = a_{ik} \qquad (i = 0,..., p^s - 1).$$

Hence for any $\theta \in$ Aut G, it follows[1] that $b^\theta \equiv b^k \bmod G'$ and so $b^\theta \equiv b^k \bmod \Phi$ for some k relatively prime to p.

Next, since $gp\{a_0, \Phi\}$ is characteristic[1] in G (see [4; 2.1]), therefore $a_0^\theta \equiv a_0^j \bmod \Phi$ for some j relatively prime to p. Noting that G is generated by b and a_0 it follows by Corollary 1 that Aut $G/\mathfrak{F}$ is Abelian and of order $\leqslant (p - 1)^2$. To complete the proof of (i) we select k and j to be primitive roots modulo p and note that in that case β^* above and α^* defined by

$$b^{\alpha^*} = b, \; a_i^{\alpha^*} = a_i^j \qquad (i = 0,..., p^s - 1)$$

are automorphisms of G which induce automorphisms of order $p - 1$ in G/Φ.

(ii): In [7; Theorem 5.1] we showed that G has nilpotency class p^s whence $\mathfrak{F}$ has class $\geqslant p^s - 1$, which is the class of the group of inner automorphisms of G.

If $s = 1$ then Γ_i/Γ_{i+1} has exponent p ($i = 1,..., p$). Hence by Theorem 3, $\mathfrak{F}$ has class $\leqslant p - 1$ and equality follows.

---

[1] This is not the case when $p = 2$, $r = s = 1$, for then G is the octic group and has an automorphism mapping b onto a_0 and a_0 onto b.

The case $s > 1$ requires a closer examination of $\mathfrak{F}$. The follow mappings of generators of G define automorphisms which generate $\mathfrak{F}$:

(I) $b \to b$, $a_0 \to a_0(a_0a_1^{-1})^{t_1} \cdots (a_{p^s-2}a_{p^s-1}^{-1})^{t_{p^s-1}}$, $0 \leqslant t_i < p$ $(i = 1,..., p^s - 1)$;

(II) $b \to b^{1+kp}$ $(0 \leqslant k < p^s)$, $a_0 \to a_0$

(III) inner automorphisms.

In (I), note that the base group $K = gp\{a_0,..., a_{p^s-1}\}$ is characteristic and hence that every Φ-automorphism maps a_0 onto a_0h with $h \in \Phi \cap K = \Gamma_2$, which is generated by $a_ia_{i+1}^{-1}$ $(i = 0,..., p^s - 2)$. In (II), $a_i \to a_{i(1+kp)}$.

It can now be verified that the derived group $\mathfrak{F}'$ of $\mathfrak{F}$ lies in the group of inner automorphisms of G and further consists entirely of Γ_3-automorphisms (This depends on the fact that $a_0a_p^{-1} \in \Gamma_3$.) Now Γ_3 has order p^{p^s-2} and hence Γ_i/Γ_{i+1} has order p for $i = 3,..., p^s$. Using Theorem 2 we deduce that $\mathfrak{F}$ has class $\leqslant p^s - 1$, and again equality follows.

We conclude with a further application of Corollary 1.

THEOREM 4. *If G is a nilpotent 2-generator group of order 2^m3^n, then Aut G is solvable.*

Proof. G is the direct product $G(2) \times G(3)$ of its Sylow subgroups and Aut G = Aut $G(2) \times$ Aut $G(3)$. It is thus sufficient to prove the theorem for 2-generator 2-groups or 3-groups. Let G be such a group. In Corollary 1 put $N = \Phi$. Since G/Φ is elementary Abelian of order 4 or 9, Aut (G/Φ) is solvable (Burnside [*1*; §311]). Hence Aut $G/\mathfrak{F}$ is solvable and since $\mathfrak{F}$ is nilpotent, therefore Aut G is solvable.

REFERENCES

1. BURNSIDE, W. "Theory of Groups of Finite Order," 2nd ed. Dover, New York, 1955.
2. HALL, MARSHALL. "The Theory of Groups." Macmillan, New York, 1959.
3. HALL, P. Nilpotent groups. *Can. Math. Congr. Summer Seminar, University of Alberta* 1957.
4. HOUGHTON, C. H. On the automorphism groups of certain wreath products. *Publ. Math. Debrecen* **9** (1962), 307-313.
5. KALOUJNINE, L. Über gewisse Beziehungen zwischen einer Gruppe und ihren Automorphismen. *Berliner Math. Tagung* (1953), 164-172.
6. LIEBECK, H. A note on prime-power groups with symmetrical generating relations. *Proc. Cambridge Phil. Soc.* **51** (1955), 394-395.
7. LIEBECK, H. Concerning nilpotent wreath products. *Proc. Cambridge Phil. Soc.* **58** (1962), 443-451.